What you want: To improve your Local Area Network.

What you get:
A superior
protocol analyzer.

The Sniffer is the only way to find *everything* on your network, at any protocol level.
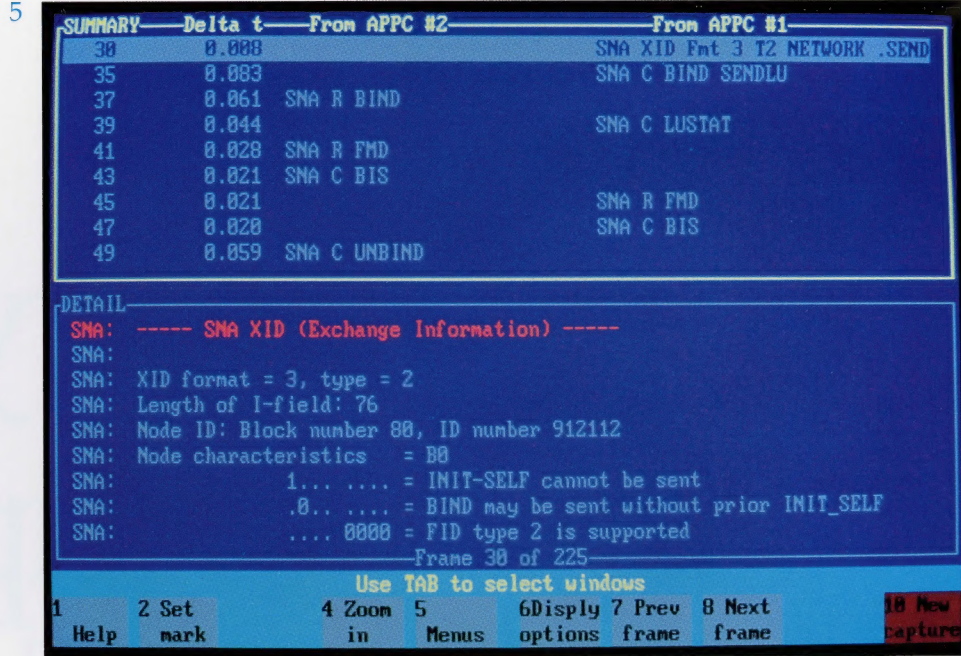
The development of The Sniffer was led by Dr. Harry Saal, one of the pioneers in Local Area Networks. In all the time he's been working with LANs, not *once* has he encountered one that was running as cleanly or as quickly as it ought to.

Nor did he encounter a protocol analyzer that could inspect *every* possible trouble spot, and deliver feedback in the same precise language you use.

Clearly, a need existed for a comprehensive LAN tester.

Here it is!

1 The Token-Ring Sniffer's™ Master Menu. Initiate Data Capture from the LAN by touching <ENTER> or by touching function key F10 as suggested by function key menu along the bottom of the screen. You can select various data display parameters from the right hand menu column. Various triggering and filtering combinations are available during capture, set up by invoking appropriate master menu selections.
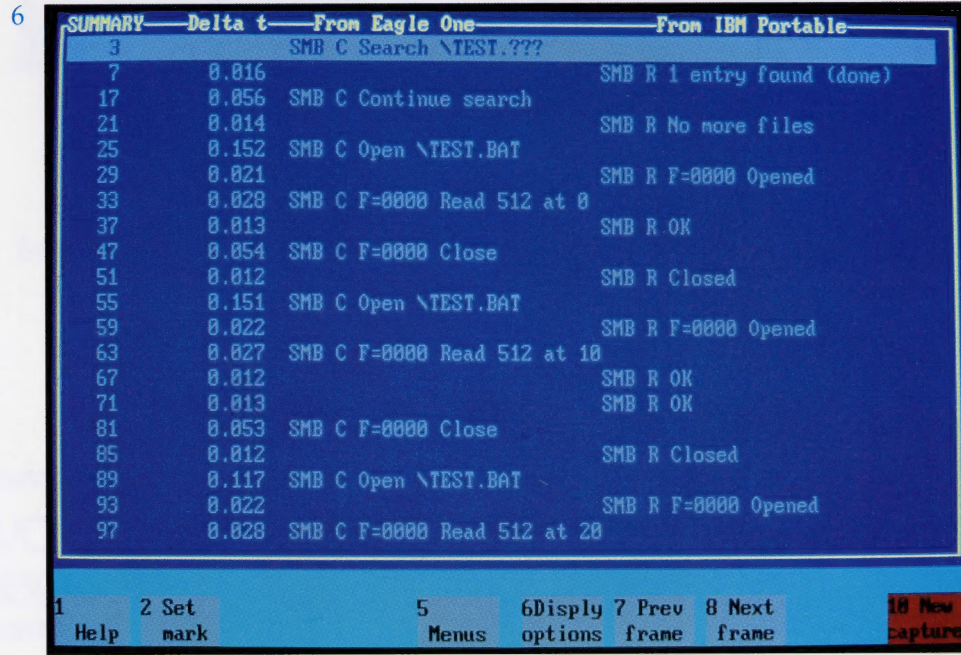
2 The Capture information display shows the current data rate (solid horizontal bar at the bottom), and the peak rate reached in this session (shaded bar). Traffic generated by each station during the session is shown in the tables at the top.

3 The Sniffer's three-window data display: a summary view of each frame at the top, with each embedded protocol summarized; expanded protocol detail translated into English in the center window; a hexadecimal dump with ASCII/EBCDIC interpretation below—note highlighting of the bytes associated with the selected detail item.
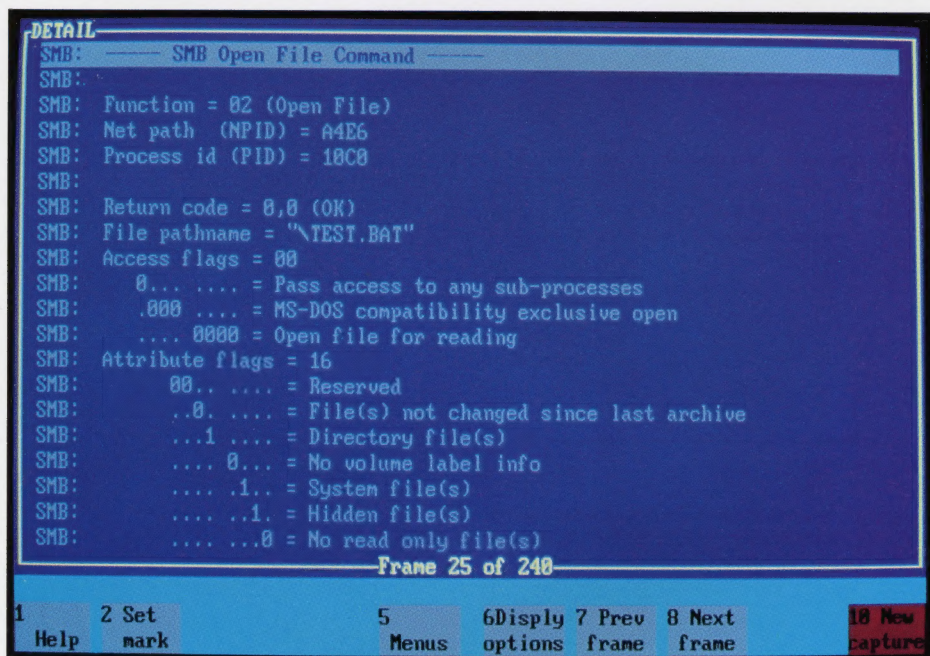
Screen 1

```
MENUS                                      More↑
                                          ▶Show frame counts
                                           Show Kbyte counts
    ┌──────────┐   Traffic Generator ◄    Show NW usage
    │ Network  │   Capture filters
    │ General  │   Trigger                Linear bar scale
    └──────────┘   Capture           ◄   ▶Log bar scale
                   Display           ◄
 Token-Ring Sniffer  Files                Individual counts
                   Exit              ◄   ▶Pair counts
 Version 1.2
                                          From <Token Ring> ◄
 (C) Copyright
 1986, 1987                               More↓

       Begin data collection from the network.
       Press ENTER to do this function

1            3 Data                                 10 New
Help         display                                capture
```

Screen 2

```
CAPTURING          Number of frames from the station    00:00:54
  Eagle One      14   Broadcast   11  This Sniffer  11  Broadcast
  IBM Portable    4   IBM Portable IBM Portable      2  LAN Manager
  IBM Portable    5   Broadcast     Eagle One       3  LAN Manager
  IBM Portable    8   Param Server  Eagle One       2  Error Mon.
  IBM Portable   23   NETBIOS

  72 frames seen.   4 Kbytes,   72 frames accepted.   2% buffer used.
                        ◄ PAUSED ►
 1       3       10      30      100     300    1000
               Frames per second
1            3 Data  4 Clear 5    6Captur        9      10 New
Help         display screen Menus options        Resume capture
```

Screen 3

```
SUMMARY───Rel time──DST────────SRC──
  55      0.041  NETBIOS   ►90005A00310A  DLC AC=10, FC=40, FS=00
                                           RI  LB FWD
                                           LLC C D=F0 S=F0 UI
                                           NET Find name CHARLOTC
  56      0.116  PC Server #1►HJS  DLC AC=10, FC=40, FS=00

DETAIL
NET: ───── NETBIOS Name Query ─────
NET:
NET: Header length = 44, Data length = 0
NET: Delimiter = EFFF (NETBIOS)
NET: Command = 0A
                        Frame 55 of 80
HEX                                                ASCII
0000 10 40 C0 00 00 00 00 00  90 00 5A 00 31 0A C2 70  .@........Z.1..p
0010 F0 F0 03 2C 00 FF EF 0A  00 AC 00 00 00 64 62 43  ...,.........dbC
0020 48 41 52 4C 4F 54 43 20  20 20 20 20 20 20 20 53  HARLOTC        S
0030 4E 41 47 41 54 45 31 37  20 20 20 20 20 20 20 20  NAGATE17
                        Frame 55 of 80
                 Use TAB to select windows
1      2 Set        4 Zoom 5       6Disply 7 Prev  8 Next   10 New
Help   mark         in     Menus   options frame  frame     capture
```

4 The Sniffer's two-viewport, multiple window display for convenient tracing or comparison of information in different frames. Note system overhead shown here: multiple inquiries regarding station EAGLE. The Sniffer is expert at revealing such inefficiencies.

5 A Summary and Detail examination selectively focused on higher level SNA protocols.

6 The two-station presentation available in The Sniffer makes it easy to track command/response situations (note 'C' and 'R' in the display), in this case DOS level SMB frames.

Screen 4

```
SUMMARY──Delta t──From IBM Portable  SUMMARY──Delta t──From IBM Portable
rtable NET Find name EAGLE<05>      00 NETBIOS  ►IBM Portable NET Fi
rtable NET Find name EAGLE<05>      99 NETBIOS  ►IBM Portable NET Fi
                                    99 NET Session alive
rtable NET Find name EAGLE<05>      00 NETBIOS  ►IBM Portable NET Fi
rtable NET Find name EAGLE<03>      04 NETBIOS  ►IBM Portable NET Fi
       NET Name EAGLE<03> recognized 11         NET Na
on initialize                       99 NET D=02 S=04 Session initialize
     NET D=04 S=02 Session confirm  10          NET D=
70 bytes                            16 NET D=02 S=04 Data, 70 bytes

DETAIL                               DETAIL
NET: ──── NETBIOS Data Only Last -   NET: ──── NETBIOS Session Initiali
NET:                                 NET:
NET: Header length = 14, Data length NET: Header length = 14, Data length
NET: Delimiter = EFFF (NETBIOS)      NET: Delimiter = EFFF (NETBIOS)
NET: Command = 16                    NET: Command = 19
NET: Transmit correlator = 0000      NET: Max data receive size = 2000
NET: Remote session number = 2       NET: Transmit correlator = 003C
NET: Local session number = 4        NET: Receive correlator = 0020
NET:                                 NET: Remote session number = 2
       Frame 65 of 84                       Frame 61 of 84
                 Use TAB to select windows
1      2 Set        4 Zoom 5       6Disply 7 Prev  8 Next   10 New
Help   mark         in     Menus   options frame  frame     capture
```

Screen 5

```
SUMMARY──Delta t──From APPC #2──────────From APPC #1──
  30     0.008                       SNA XID Fmt 3 T2 NETWORK .SEND
  35     0.003                       SNA C BIND SENDLU
  37     0.061 SNA R BIND
  39     0.044                       SNA C LUSTAT
  41     0.028 SNA R FMD
  43     0.021 SNA C BIS
  45     0.021                       SNA R FMD
  47     0.020                       SNA C BIS
  49     0.059 SNA C UNBIND

DETAIL
SNA: ───── SNA XID (Exchange Information) ─────
SNA:
SNA: XID format = 3, type = 2
SNA: Length of I-field: 76
SNA: Node ID: Block number 80, ID number 912112
SNA: Node characteristics = B0
SNA:    1... .... = INIT-SELF cannot be sent
SNA:    .0.. .... = BIND may be sent without prior INIT_SELF
SNA:    .... 0000 = FID type 2 is supported
                        Frame 30 of 225
                 Use TAB to select windows
1      2 Set        4 Zoom 5       6Disply 7 Prev  8 Next   10 New
Help   mark         in     Menus   options frame  frame     capture
```

Screen 6

```
SUMMARY──Delta t──From Eagle One─────────From IBM Portable──
   3                  SMB C Search \TEST.???
   7    0.016                       SMB R 1 entry found (done)
  17    0.056  SMB C Continue search
  21    0.014                       SMB R No more files
  25    0.152  SMB C Open \TEST.BAT
  29    0.021                       SMB R F=0000 Opened
  33    0.028  SMB C F=0000 Read 512 at 0
  37    0.013                       SMB R OK
  47    0.054  SMB C F=0000 Close
  51    0.012                       SMB R Closed
  55    0.151  SMB C Open \TEST.BAT
  59    0.022                       SMB R F=0000 Opened
  63    0.027  SMB C F=0000 Read 512 at 10
  67    0.012                       SMB R OK
  71    0.013                       SMB R OK
  81    0.053  SMB C F=0000 Close
  85    0.012                       SMB R Closed
  89    0.117  SMB C Open \TEST.BAT
  93    0.022                       SMB R F=0000 Opened
  97    0.028  SMB C F=0000 Read 512 at 20

1      2 Set             5         6Disply 7 Prev  8 Next   10 New
Help   mark              Menus     options frame  frame     capture
```

Color display is available only with an external monitor.

7
```
DETAIL
SMB: ———— SMB Open File Command ————
SMB:
SMB: Function = 02 (Open File)
SMB: Net path  (NPID) = A4E6
SMB: Process id (PID) = 18C0
SMB:
SMB: Return code = 0,0 (OK)
SMB: File pathname = "\TEST.BAT"
SMB: Access flags = 00
SMB:      0... .... = Pass access to any sub-processes
SMB:      .000 .... = MS-DOS compatibility exclusive open
SMB:      .... 0000 = Open file for reading
SMB: Attribute flags = 16
SMB:      00.. .... = Reserved
SMB:      ..0. .... = File(s) not changed since last archive
SMB:      ...1 .... = Directory file(s)
SMB:      .... 0... = No volume label info
SMB:      .... .1.. = System file(s)
SMB:      .... ..1. = Hidden file(s)
SMB:      .... ...0 = No read only file(s)
                    Frame 25 of 248
1        2 Set                    5      6Disply 7 Prev  8 Next     10 New
Help     mark                     Menus  options frame   frame      capture
```
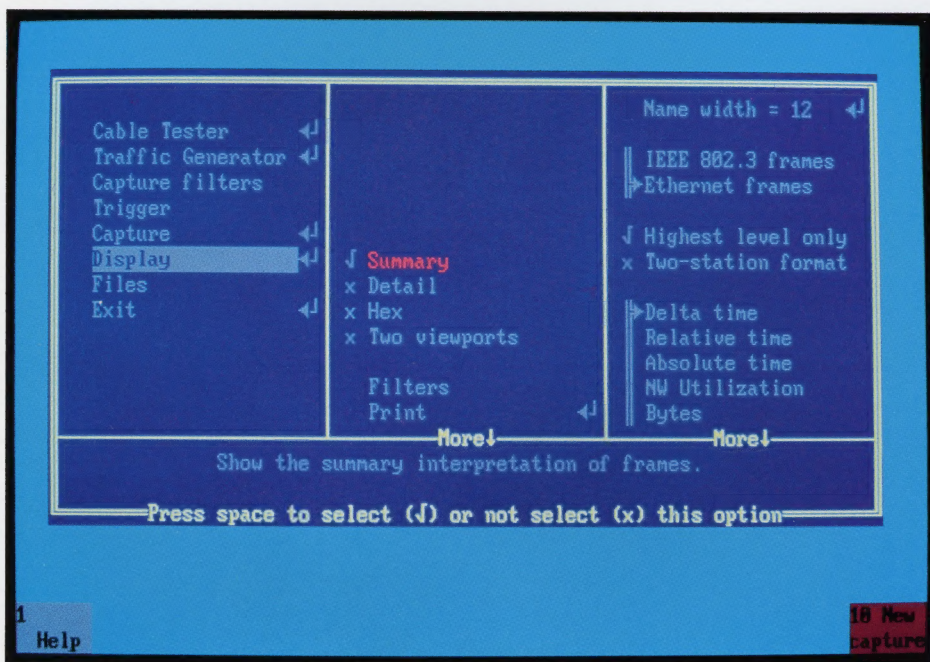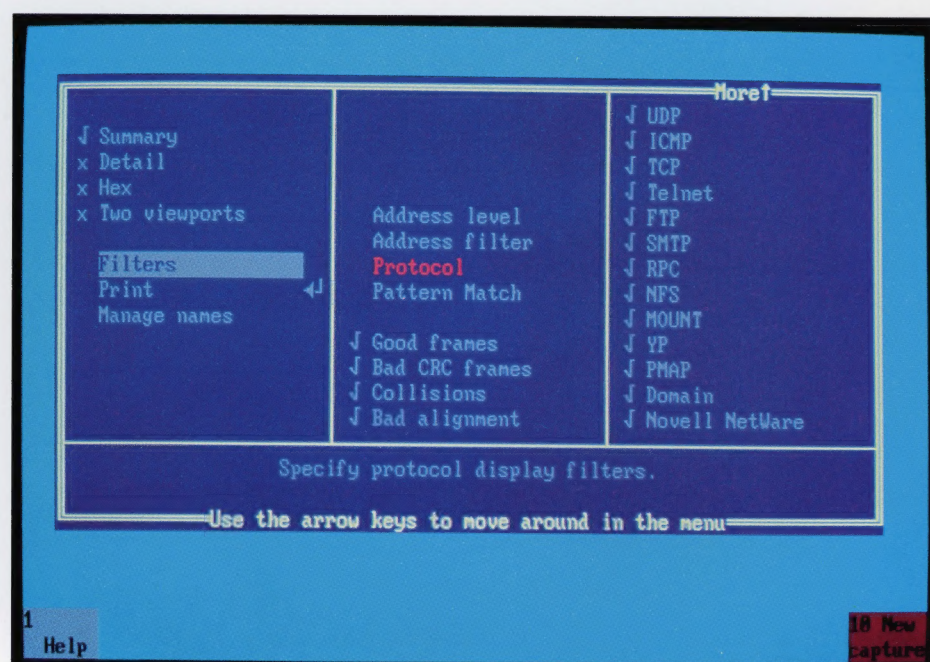
7 A Detail view of an SMB 'Open File' command.
8 The Display/Summary sub-menu of the Ethernet model of The Sniffer. Persons with good LAN knowledge usually feel at home with The Sniffer's menu structure after just a few minutes of experimentation.
9 The Sniffer's Ethernet/Display/Filters/Protocols selection sub-menu area—one scrolls up and down in the right hand column to select the desired protocol filters (there are still others above and below those shown).
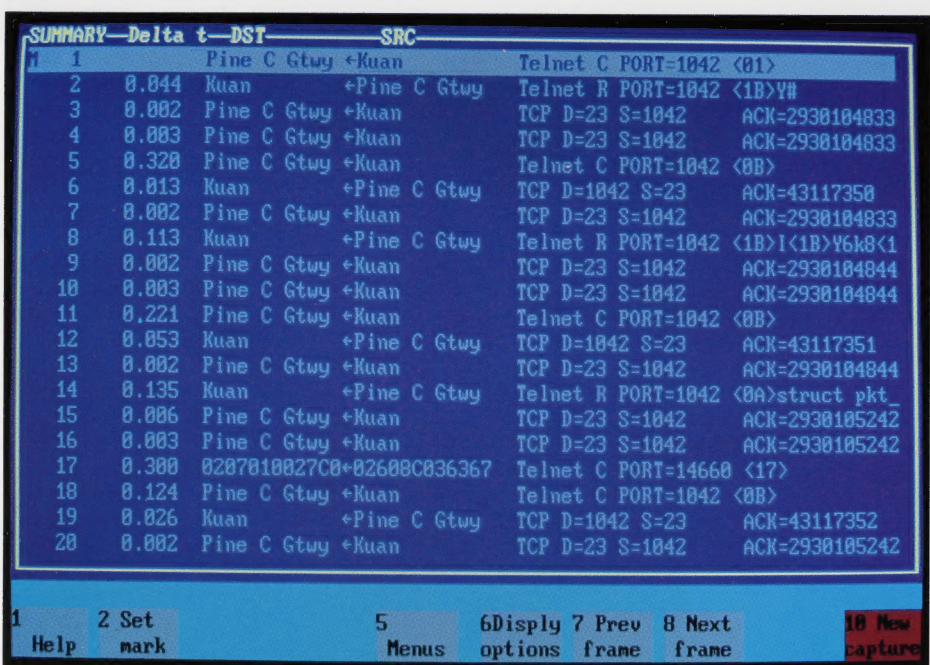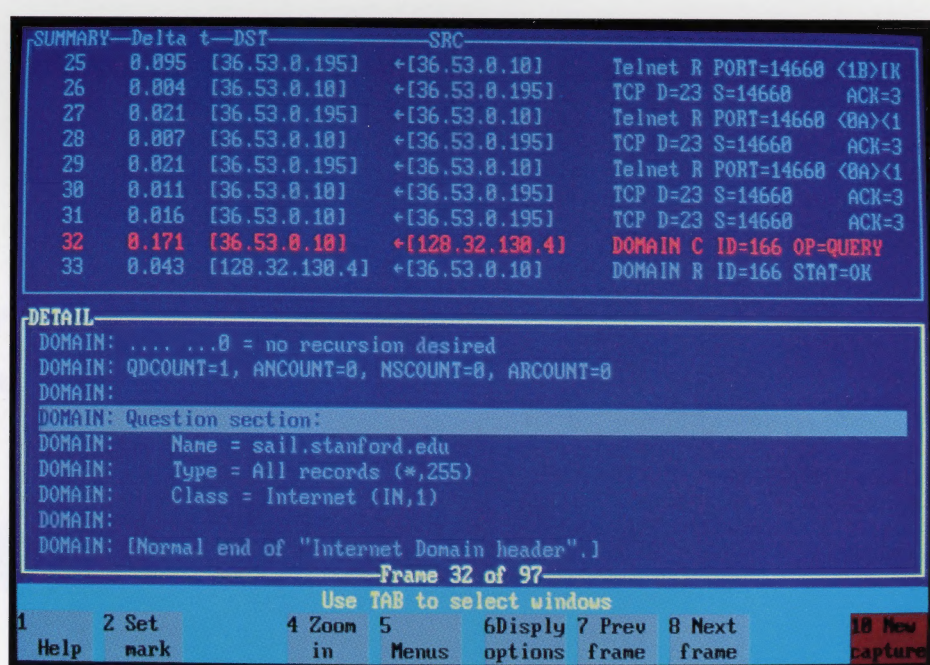
8
```
                                         Name width = 12       ↵
  Cable Tester          ↵
  Traffic Generator     ↵                ↵ IEEE 802.3 frames
  Capture filters                        ►Ethernet frames
  Trigger
  Capture               ↵                ↵ Highest level only
  Display               ↵    ↵ Summary   x Two-station format
  Files                 ↵    x Detail
  Exit                  ↵    x Hex       ►Delta time
                             x Two viewports  Relative time
                                              Absolute time
                             Filters          NW Utilization
                             Print      ↵     Bytes
                        More↓                  More↓
          Show the summary interpretation of frames.
  Press space to select (√) or not select (x) this option
1
Help                                                        10 New
                                                            capture
```

9
```
                                                        More↑
  √ Summary                                    √ UDP
  x Detail                                     √ ICMP
  x Hex                                        √ TCP
  x Two viewports           Address level      √ Telnet
                            Address filter     √ FTP
  Filters                   Protocol           √ SMTP
  Print                ↵    Pattern Match      √ RPC
  Manage names                                 √ NFS
                                               √ MOUNT
                            √ Good frames       √ YP
                            √ Bad CRC frames    √ PMAP
                            √ Collisions        √ Domain
                            √ Bad alignment     √ Novell NetWare
                     Specify protocol display filters.
           Use the arrow keys to move around in the menu
1
Help                                                        10 New
                                                            capture
```

10
```
SUMMARY—Delta t—DST———      —SRC———
M  1        Pine C Gtwy ←Kuan          Telnet C PORT=1042 <01>
   2  0.044 Kuan          ←Pine C Gtwy Telnet R PORT=1042 <1B>V#
   3  0.002 Pine C Gtwy ←Kuan          TCP D=23 S=1042      ACK=2930104833
   4  0.003 Pine C Gtwy ←Kuan          TCP D=23 S=1042      ACK=2930104833
   5  0.320 Pine C Gtwy ←Kuan          Telnet C PORT=1042 <0B>
   6  0.013 Kuan          ←Pine C Gtwy TCP D=1042 S=23      ACK=43117350
   7  0.002 Pine C Gtwy ←Kuan          TCP D=23 S=1042      ACK=2930104833
   8  0.113 Kuan          ←Pine C Gtwy Telnet R PORT=1042 <1B>I<1B>Y6k8<1
   9  0.002 Pine C Gtwy ←Kuan          TCP D=23 S=1042      ACK=2930104844
  10  0.003 Pine C Gtwy ←Kuan          TCP D=23 S=1042      ACK=2930104844
  11  0.221 Pine C Gtwy ←Kuan          Telnet C PORT=1042 <0B>
  12  0.053 Kuan          ←Pine C Gtwy TCP D=1042 S=23      ACK=43117351
  13  0.002 Pine C Gtwy ←Kuan          TCP D=23 S=1042      ACK=2930104844
  14  0.135 Kuan          ←Pine C Gtwy Telnet R PORT=1042 <0A>struct pkt_
  15  0.006 Pine C Gtwy ←Kuan          TCP D=23 S=1042      ACK=2930105242
  16  0.003 Pine C Gtwy ←Kuan          TCP D=23 S=1042      ACK=2930105242
  17  0.300 0207010027C8←02608C036367  Telnet C PORT=14660 <17>
  18  0.124 Pine C Gtwy ←Kuan          Telnet C PORT=1042 <0B>
  19  0.026 Kuan          ←Pine C Gtwy TCP D=1042 S=23      ACK=43117352
  20  0.002 Pine C Gtwy ←Kuan          TCP D=23 S=1042      ACK=2930105242
1        2 Set                    5      6Disply 7 Prev  8 Next     10 New
Help     mark                     Menus  options frame   frame      capture
```

11
```
SUMMARY—Delta t—DST———        —SRC———
  25  0.095 [36.53.0.195]  ←[36.53.0.10]   Telnet R PORT=14660 <1B>IK
  26  0.004 [36.53.0.10]   ←[36.53.0.195]  TCP D=23 S=14660      ACK=3
  27  0.021 [36.53.0.195]  ←[36.53.0.10]   Telnet R PORT=14660 <0A>{1
  28  0.007 [36.53.0.10]   ←[36.53.0.195]  TCP D=23 S=14660      ACK=3
  29  0.021 [36.53.0.195]  ←[36.53.0.10]   Telnet R PORT=14660 <0A>{1
  30  0.011 [36.53.0.10]   ←[36.53.0.195]  TCP D=23 S=14660      ACK=3
  31  0.016 [36.53.0.10]   ←[36.53.0.195]  TCP D=23 S=14660      ACK=3
  32  0.171 [36.53.0.10]   ←[128.32.130.4] DOMAIN C ID=166 OP=QUERY
  33  0.043 [128.32.130.4] ←[36.53.0.10]   DOMAIN R ID=166 STAT=OK
DETAIL
DOMAIN: ..... ...0 = no recursion desired
DOMAIN: QDCOUNT=1, ANCOUNT=0, NSCOUNT=0, ARCOUNT=0
DOMAIN:
DOMAIN: Question section:
DOMAIN:     Name = sail.stanford.edu
DOMAIN:     Type = All records (*,255)
DOMAIN:     Class = Internet (IN,1)
DOMAIN:
DOMAIN: [Normal end of "Internet Domain header".]
                    Frame 32 of 97
                Use TAB to select windows
1        2 Set       4 Zoom  5      6Disply 7 Prev  8 Next     10 New
Help     mark         in    Menus  options frame   frame      capture
```

10 Here's a Display/Summary window with an example of repetitive acknowledgements—not uncommon on networks we have seen—but often a waste of time and resources. Use The Sniffer to track down and eliminate these inefficiencies—get more out of your network investment.

11 Illustrating how The Sniffer can look behind the gateway in an Ethernet environment, by showing addresses imbedded in higher level protocols.
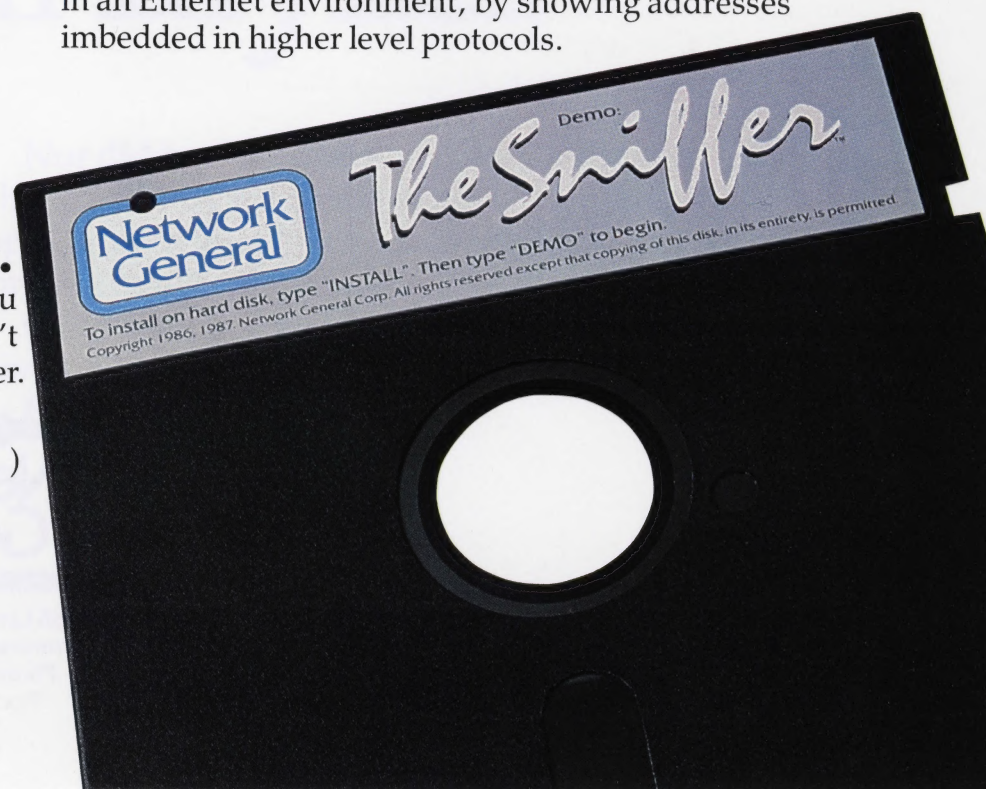
Network General

1296B Lawrence Station Road
Sunnyvale, California 94089
Phone: (408) 734-0464
Fax: (408) 734-1828